Efficiency Evaluating of the Security Components of Computer Systems

Anatoliy Ihnatovych

Department of Computer Engineering, Lviv Polytechnic National University, UKRAINE, Lviv, S. Bandery Street 12, e-mail: ignatovicha@gmail.com

Abstract – This research work proposes a general theoretical model of efficiency evaluating of the security components of computer systems. Efficiency complexity is overviewed and various components of efficiency evaluation are defined and there dimensions are derived.

Key words: security components, cryptography, effectiveness, efficiency.

I. Introduction

Any of newly introduced or designed security components of computer systems require evaluation of their efficiency and effectiveness. To obtain the most objective results it is expedient to carry out efficiency evaluation comparing exclusively the same type of computer system security components.

For instance, many experts of the cryptographic community evaluate the efficiency of encryption systems by the number of keys that can be provided by the system. In certain cases the time to "crack" the encryption system using modern technology and software solutions is calculated. In some cases it is suggested to take into account the cost for breaking into a secured computer system compared to the cost of encrypted information [1 – 4].

As the technical parameters of computational and mathematical tools are changing faster than above mentioned evaluation results are published, it is obvious that it is necessary to find such approaches for efficiency evaluating, which would not depend on time, actual level of computer technologies development and other factors influence.

Task complexity is to find a universal approach of efficiency determination uniting various by nature, dimension, and physical quantities types of parameters.

II. Efficiency evaluating indicator of the security components of computer systems

Whatsoever of technical parameters that describes various values is desirable to measure in numerical a numerical or other measurable form (in case it is possible to evaluate in such a way).

Therefore unspecified efficiency of the security components of computer systems can be measured by the efficiency indicator E which is the function of a set of performance indicators E_i:

$$E = f\left(E_i\right),\ i = \overline{1,n}, \tag{1}$$

where n – general quantity of efficiency evaluating criteria, which are used for evaluation of generalized efficiency evaluating indicator.

Nowadays there is no universally accepted and standardized analytical expression for the efficiency evaluating of security components of computer systems. One of the objectification of such indicator/ assessment can be a mathematician expression

$$E = \left(\sum_{j=1}^{n} E_j\right) : n,\ j = \overline{1,n}\ , \tag{2}$$

where E_j – parameter which is determined as a relative normalized value of j efficiency evaluating indicator that can go up to a maximum value 1.

Normalized value of efficiency evaluating indicator can be calculated using formula (3):

$$E = \frac{E_{jo}}{E_{jm}}, \tag{3}$$

where E_{jo} – calculated j efficiency evaluating indicator for a particular safety mean; E_{jm} – maximum (or optimum) value of j efficiency evaluating indicator.

Performance indicators can be direct when increasing of their value leads to improve of performance, or inverse when reduction of their value leads to increase of efficiency of security components. Therefore, assessing the effectiveness it is necessary to determine whether direct or inverse efficiency evaluation indicators are used.

The most widespread Efficiency evaluating indicators include the following:

E1 – reliability of used devices/tools;

E2 – sustainability of cryptographic tools;

E3 – productivity when working with security components;

E4 – evaluation of the average frequency integrated deviation of symbols usage for the specific security component;

E5 – probability of reducing of the frequency of repetitions in the ciphertext that corresponds to the repetition of plaintext;

E6 – number of possible key sets;

E7 – the ratio of the value of security component to the value of the protected product.

The main features of these indicators could be described as:

E1 – reliability of the used components is determined by the security features of the used algorithm, possibilities of its modifications, the complexity of mathematical transformations and calculations, ease of usage (elimination of errors during the work).

E2 – resistance of cryptographic tools is determined by time, which is necessary to expose the key and the encrypted text using available tools (computers, software, qualified specialists).

E3 – effectiveness of security components is determined by the time, which is used by system administrator for administration of security components.

E4 – evaluation of decreasing of the average frequency integrated deviation of symbols usage for the specific security component.

E5 – probability of reducing of the frequency of repetitions in the ciphertext that corresponds to the repetition of plaintext.

E6 – number of possible key sets is one of the main factors determining the resistance of cryptographic tools. Simultaneously it is necessary to take into consideration that near to unlimited set of keys causes problems for their processing. Also the limited number of difficult key choices by certain rules makes key-selection difficult.

E7 – the ratio of the value of security component to the value of the protected product is determined by the number of cryptographer employees, the cost of additional equipment, time that is spent for the implementation of protective functions.

In addition to above mentioned efficiency evaluation indicators there are several additional criteria that should be analyzed during selection of information security tools. For instance, an important efficiency indicator is the rate of changing keys both on the side of a transmitter and receiver (taking into account the problems of synchronization used keys). Also it is necessary to consider the hardware requirement options (RAM, operating system, speed, applied mathematical software, etc). In some cases, the amount of labour costs for preparation of the data should be considered. Thus, only in each specific case we can determine priorities and choose effective options that should be analyzed and considered.

No doubt each individual case the usage of security components differs. While efficiency evaluation some parameters/indicators, which are unimportant for a particular situationa, could be excluded simultaneously with addition of more valuable indicators. It is reasonable to consider different approaches to the construction of indicators that affect performance into one logical set.

These approaches (normalized value of efficiency, various dependences, "mirror inversion," "multiplicative inversion", usage of priority levels, usage of peer reviews etc) allow to evaluate in one set incompatible values.

Conclusion

Thus, the efficiency is a complex indicator and its usage for the classification of efficiency evaluating of security components requires specifying multiplicity of indicators.

Using the same means of protection (security components) in different operating conditions the efficiency indicator will differ. As a rule, priorities must be provided by the customer, and his assessment should be always predominant. The customer finally decides which security components should prevail and determines the value of effectiveness for the security component.

Taking into account customer priorities, the proposed efficiency evaluating indicator can be calculated by the following expression:

$$E = \left(\sum_{j=1}^{n} P_j \cdot E_j \right) : n,\ j = \overline{1,n}, \qquad (4)$$

where P_j – level of customer priority that can vary from 0 to 1, prioritizing different components of security; n – quantity of considered criteria.

When we use encryption as a one of security components, efficiency determining will be more objective if we compare the known encryption device with evaluated device. Herewith there are some advisable initial conditions necessary for obtaining a better result. These conditions include usage of the same plaintext, encryption algorithms of the same class/type, and similar technology base (computers, operating systems, applications etc).

The proposed efficiency evaluating indicator was used for efficiency evaluating of the new method of information encrypting [4, 5] based on usage of masking characters which are placed into the set of characters of plaintext before encryption. Thus it could be used for efficiency evaluating of the security components of computer systems

References

[1] Kononova V. O. Otsinka zasobiv zakhystu informatsiinykh resursiv / V. O. Kononova, O. V. Kharkianen, Hrybkov S. V. // Visnyk NU "Lvivska politekhnika" "Kompiuterni systemy ta merezhi". – 2014. – № 806. – S. 99–105.

[2] Stallings W. Computer security: principles and practice / William Stallings, Lawrie Brown. – 2nd ed. – Pearson. – 2012. – 817 p.

[3] ISO/IEC 27001 – Information security management [Electronic resource], https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en.

[4] Yakymenko I. Z. Analiz efektyvnosti zakhystu informatsii na osnovi kryptohrafichnykh peretvoren z vykorystanniam maskovanoho predstavlennia danykh / Yakymenko I. Z., Bozhyk S. V. // ACIT'5. "Suchasni komp'iuterni informatsiini tekhnolohii". TNEU. – Ternopil. 22–23 travnia 2015. – C. 182–184.

[5] Sposib shyfruvannia informatsii. Patent Ukrainy na korysnu model №99073. Biul. № 9 vid 12.05.2015. Ihnatovych A. O., Ivantsiv V. R., Ivantsiv R-A. D., Pavych N. Ia.

[6] Ihnatovych A., Pavych N. Modeli pidvyshchennia efektyvnosti ta nadiinosti blokovykh shyfriv// Zbirnyk naukovykh prats. Visnyk Lvivskoho derzhavnoho universytetu bezpeky zhyttiediialnosti, № 11 (2015). – S. 101–110.